WHAT IS CLAIMED IS:

1. A system for performing security operations on network data, the system comprising:

memory;

a data coprocessor configured to transfer data into and out of the memory;

a plurality of processors coupled to the memory and to the data coprocessor, each processor being configured to perform, in parallel to one another, security operations on a portion of the data; and

a plurality of security coprocessors coupled to the memory, each security coprocessor being coupled to a respective one of the processors and configured to assist the respective processor in performing security operations on the portion of the data.

2. The system of claim 1, wherein each of the plurality of processors comprises:

logic configured to identify a security association related to the portion of the data;

logic configured to filter the portion of the data based on the identified security association;

logic configured to divide the portion of the data into fragments and to reassemble the fragments into the portion; and

logic configured to identify a sequence associated with the portion of the data.

3. The system of claim 1, wherein each security coprocessor comprises:

logic configured to obscure the portion of the data when the portion is non-secure data;

logic configured to decipher the portion of the data when the portion is secure data;

logic configured to determine an integrity of the portion of the data; and

logic configured to establish a security association related to the portion of the data, wherein the security association includes information used to obscure and decipher the portion and to determine the integrity of the portion.

4. The system of claim 1, comprising:

a search engine coprocessor coupled to the memory and to the plurality of processors, the search engine coprocessor being configured to exchange control information between at least one of the memory and external system memory and each of the plurality of processors for use in performing security operations on the data.

5. The system of claim 4, comprising:

a memory coprocessor coupled to the plurality of processors, the memory, and the external system memory, the memory coprocessor configured to determine a status of the memory and the external system memory.

6. The system of claim 1, wherein each of the plurality of processors is further configured to perform, in parallel to one another, quality-of-service (QoS) operations on the portion of the data in coordination with performing the security operations.

7. The system of claim 6, wherein each of the plurality of processors comprises:

logic configured to identify an information flow associated with the data;

logic configured to determine a priority of the information flow; and

logic configured to manage the transfer of data into and out of the memory based on the priority of the information flow associated with the data.

8. The system of claim 7, comprising at least one of:

an enqueue coprocessor coupled to the plurality of processors and to the data coprocessor, the enqueue coprocessor configured to manage the information flow associated with the data external to the system;

a policy coprocessor configured to assist the plurality of processors in managing the transfer of the data into and out of the memory by enforcing policies of the information flow associated with the data; and

a counter coprocessor configured to provide statistics related to the transfer of the data into and out of the memory and the enforcing of policies of the information flow.

9. The system of claim 1, wherein each of the plurality of processors is configured to execute programmable instructions for performing the security operations on the portion of the data from a plurality of independent instruction streams, and can switch between instruction steams in a single clock cycle.

10. The system of claim 9, wherein each of the plurality of security processors includes separate queues corresponding to each of the independent instruction streams.

11. The system of claim 1, wherein each of the plurality of processors comprises:

logic configured to compress the portion of the data prior to performing the security operations when the portion is non-secure data; and

logic configured to decompress the portion of the data after performing the security operations when the portion is secure data.

12. The system of claim 11, wherein each security processor is configured to assist the respective processor in compressing and decompressing the portion of the data.

13. A method for performing security operations on network data, the method comprising:

transferring data into memory;

performing security operations on respective portions of the data in parallel using a plurality of processors;

using a plurality of security coprocessors to assist in performing the security operations on the respective portions of the data, each security coprocessor being coupled to a respective one of the processors; and

transferring the operated-on portions of the data out of the memory.

14. The method of claim 13, wherein the security operations performed by each of the processors comprise:

identifying a security association related to a portion of the data;

filtering the portion of the data based on the identified security association;

dividing the portion of the data into fragments;

reassembling the fragments into the portion of data; and

identifying a sequence associated with the portion of the data.

15. The method of claim 13, wherein the security operations assisted by each of the security coprocessors comprise:

obscuring a portion of the data when the portion is non-secure data;

deciphering the portion of the data when the portion is secure data;

determining an integrity of the portion of the data; and

establishing a security association related to the portion of the data, wherein the security association includes information used in obscuring and deciphering the portion and in determining the integrity of the portion.

16. The method of claim 13, comprising:

exchanging control information between at least one of the memory and external system memory and each of the plurality of processors for use in performing security operations on the data.

17. The method of claim 13, comprising:

performing quality-of-service (QoS) operations on the respective portions of the data in parallel using the plurality of processors in coordination with performing the security operations.

18. The method of claim 17, wherein the QoS operations performed by each of the processors comprise:

identifying an information flow associated with the data;

determining a priority of the information flow; and

managing the transfer of data into and out of the memory based on the priority of the information flow associated with the data.

19. The method of claim 18, comprising:

managing the information flow after transferring the operated-on portions of the data associated with the information flow out of the memory;

enforcing policies of the information flow associated with the data; and

providing statistics related to the transfer of the data into and out of the memory and the enforcing of policies of the information flow.

20. The method of claim 13, comprising:

compressing the respective portions of the data prior to performing the security operations when the portions are non-secure data; and

decompressing the respective portions of the data after performing the security operations when the portions are secure data.

21. The method of claim 13, comprising:

using each security processor to assist the respective processor in compressing and decompressing the portions of the data.

22. A computer readable medium containing a computer program for performing security operations on network data, wherein the computer program comprises executable instructions for:

transferring data into memory;

performing security operations on respective portions of the data in parallel using a plurality of processors;

using a plurality of security coprocessors to assist in performing the security operations on the respective portions of the data, each security coprocessor being coupled to a respective one of the processors; and

transferring the operated-on portions of the data out of the memory.

23. The computer readable medium of claim 22, wherein the instructions for performing security operations on respective portions of the data in parallel using a plurality of processors comprise executable instructions for:

identifying a security association related to a portion of the data;

filtering the portion of the data based on the identified security association;

dividing the portion of the data into fragments;

reassembling the fragments into the portion of data; and

identifying a sequence associated with the portion of the data.

24. The computer readable medium of claim 22, wherein the instructions for using a plurality of security coprocessors to assist in performing the security operations comprise executable instructions for:

obscuring a portion of the data when the portion is non-secure data;

deciphering the portion of the data when the portion is secure data;

determining an integrity of the portion of the data; and

establishing a security association related to the portion of the data, wherein the security association includes information used in obscuring and deciphering the portion and in determining the integrity of the portion.

25. The computer readable medium of claim 22, wherein the computer program comprises executable instructions for:

exchanging control information between at least one of the memory and external system memory and each of the plurality of processors for use in performing security operations on the data.

26. The computer readable medium of claim 22, wherein the computer program comprises executable instructions for:

performing quality-of-service (QoS) operations on the respective portions of the data in parallel using the plurality of processors in coordination with performing the security operations.

27. The computer readable medium of claim 26, wherein the instructions for performing QoS operations on the respective portions of the data in parallel using the plurality of processors in coordination with performing the security operations comprise executable instructions for:

identifying an information flow associated with the data;

determining a priority of the information flow; and

managing the transfer of data into and out of the memory based on the priority of the information flow associated with the data.

28. The computer readable medium of claim 27, wherein the computer program comprises executable instructions for:

managing the information flow after transferring the operated-on portions of the data associated with the information flow out of the memory;

enforcing policies of the information flow associated with the data; and

providing statistics related to the transfer of the data into and out of the memory and the enforcing of policies of the information flow.

29. The computer readable medium of claim 22, wherein the computer program comprises executable instructions for:

compressing the respective portions of the data prior to performing the security operations when the portions are non-secure data; and

decompressing the respective portions of the data after performing the security operations when the portions are secure data.